BAB III

METODELOGI PENELITIAN

3.1 Studi Literatur

Mempelajari literatur dan mencari informasi dari jurnal, skripsi dan sumber lainnya yang berkaitan dengan teknik kriptografi terutama mengenai enkripsi algoritma blowfish.

3.2 Analisis Permasalahan

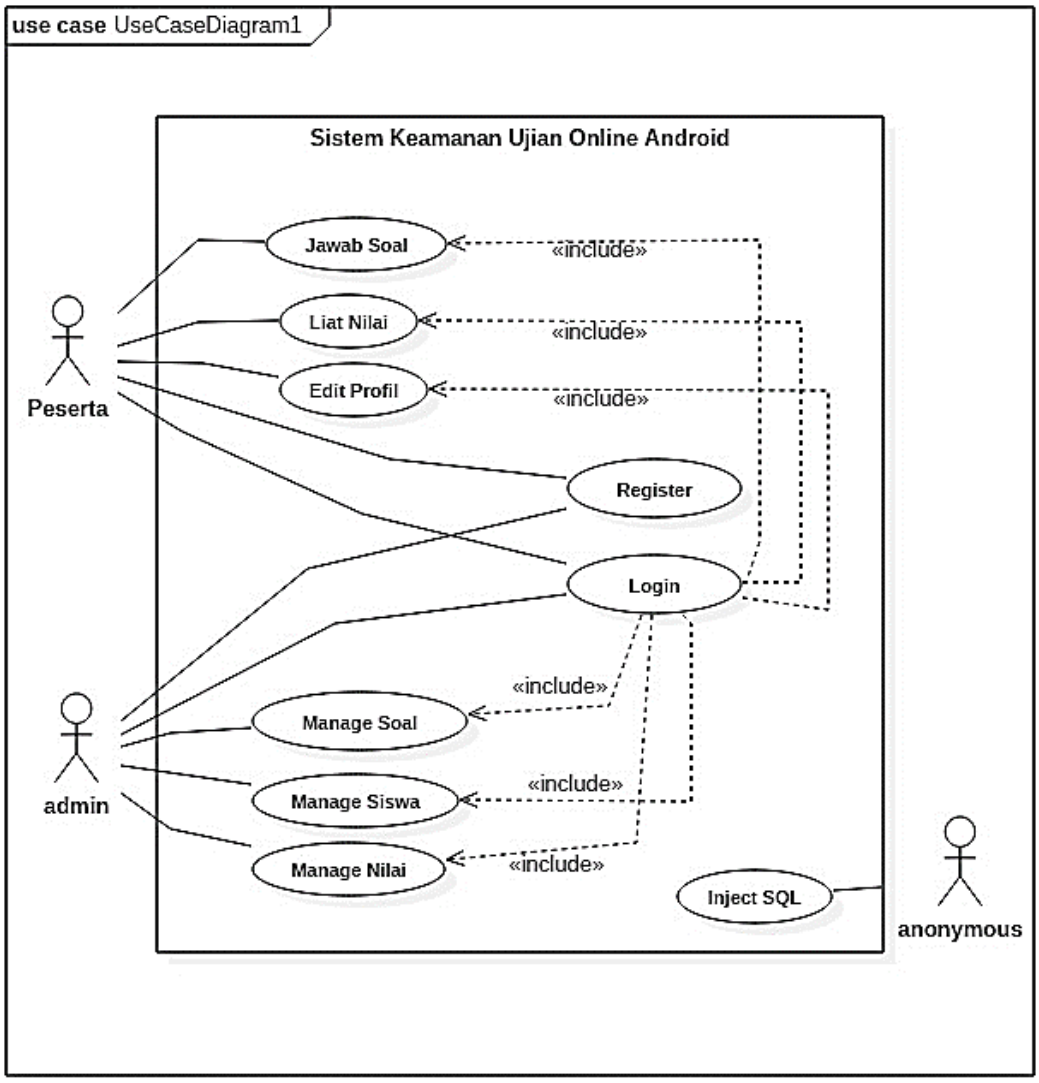
Dalam analisis permasalahan dapat diketahui bahwa keamanan di dalam pelaksanaan ujian *online* masih rentan terhadap adanya gangguan dari pihak lain. Masalah keamanan yang dapat terjadi ketika nilai peserta ujian yang telah tersimpan dalam *database* ujian dapat diketahui pihak lain sehingga mengurangi privasi terhadap kepemilikan nilai dari peserta yang sebenarnya. Selain itu modifikasi terhadap nilai peserta juga dapat dilakukan jika tidak adanya pengamanan

3.3 Analisis Kebutuhan Fungsional

Kebutuhan fungsional adalah pernyataan-pernyataan apa saja yang sistem harus lakukan dan layanan-layanan apa yang dapat diberikan sistem kepada pengguna (Inggrita Mahardika Pratama 2017)

3.3.1 *Use Case* Diagram

Use Case Diagram merupakan salah satu model UML yang digunakan untuk mendeskripsikan kebutuhan fungsional sebuah sistem dari sisi aktor, tujuan aktor, dan hal yang berkaitan antara keduanya. *Use case* diagram juga menunjukan perilaku (*behavior*) dari sistem yang akan dibuat. Diagram *use case* pada sistem ini dapat dilihat dalam gambar 3.1



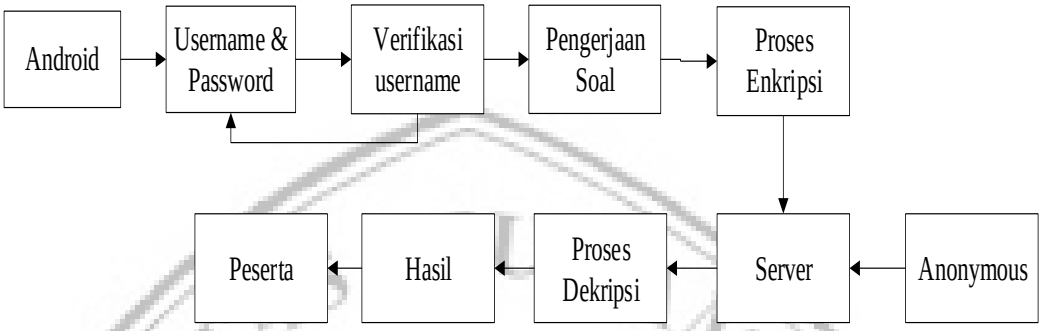
Gambar 3.1 *Use Case* Diagram Sistem Keamanan Ujian *Online*

Penjelasan *use case* diagram:

- *Use case* peserta: merupakan penjelasan peserta ujian sebagi user dengan hak akses login, registrasi, jawab soal, lihat nilai, dan edit profil.
- *Use case* admin: Use case admin melakukan fungsi control terhadap database ujian seperti manage peserta, manage nilai, maupun soal.
- *Use case* anonymous: merupakan orang yang melakukan aksi hacking di form login admin menggunakan SQL *injection*.

3.4 Perancangan Sistem

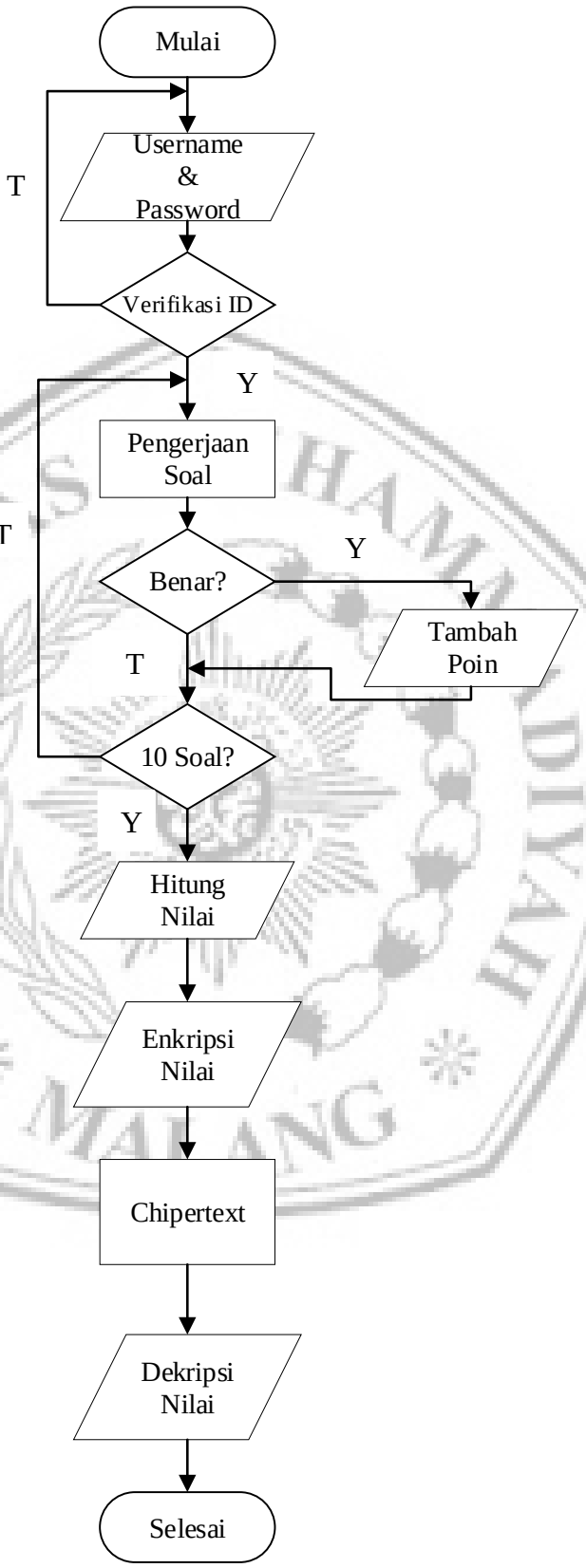
Berikut diagram blok perancangan sistem keamanan ujian online menggunakan algoritma enkripsi Blowfish disajikan pada gambar 3.2



Gambar 3.2 Diagram Blok Perancangan Sistem

Pada Gambar 3.2 Menjelaskan peserta sebagai peserta menjalankan aplikasi ujian pada *smartphone* untuk menjawab soal ujian. Sebelumnya peserta ujian *online* memasukkan *username* dan *password*. Jika *username* peserta salah maka peserta akan melakukan *login* kembali, dan jika *username* peserta benar maka sistem akan menampilkan soal ujian. Setelah itu sistem melakukan perlindungan enkripsi menggunakan metode blowfish terhadap keamanan nilai sebagai data *input* ke dalam *database*. Setelah pengolahan data input, sistem melakukan dekripsi terhadap *ciphertext* nilai agar peserta dapat melihat hasil dari ujian online yang dikerjakan. Di dalam sistem ujian *online* tersebut juga terdapat seseorang sebagai *anonymous* yang menyerang form login admin menggunakan teknik SQL Injection untuk masuk ke dalam *database* dengan tujuan dapat mengubah nilai dari peserta.

Berikut ini adalah perancangan pembuatan program aplikasi dalam bentuk *flowchart.*



Gambar 3.3 *Flowchart* Perancangan Sistem

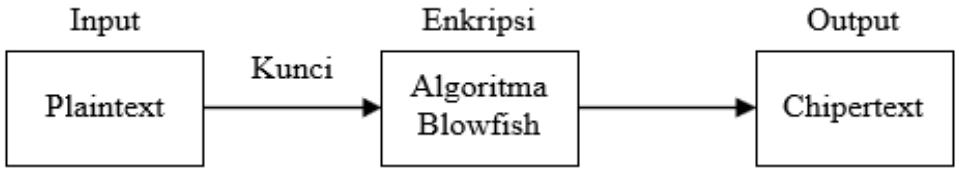
Pada gambar 3.3 dijelaskan bahwa sistem dimulai dari *login* dengan memasukkan *username* dan *password*. Setelah login peserta mengerjakan soal ujian. Setiap jawaban benar akan ada penambahan poin kemudian setelah mengerjaakan 10 soal, nilai akan dihitung (poin/10 dikalikan 100). Selanjutnya nilai akan di enkripsi menjadi chipertext/pesan yang tidak bisa di ketahui. Setelah itu dilakukan dekripsi untuk melihat nilaia asli peserta ujian.

3.5 Perancangan Sistem dengan Algoritma Blowfish

Pada tahap ini akan dirancang sistem untuk enkripsi dan dekripsi nilai ujian menggunakan algoritma blowfish.

3.5.1 Proses Enkripsi

Berikut adalah diagram blok proses enkripsi nilai ujian:



Gambar 3.4 Diagram Blok Proses Enkripsi Nilai Ujian *Online*

Pada gambar 3.4 dijelaskan bahwa proses enkripsi dimulai dengan memasukkan *plaintext* yaitu nilai peserta ujian. Kemudian akan dilakukan enkripsi dengan algoritma blowfish menggunakan kunci enkripsi. Selanjutnya setelah proses enkripsi berhasil maka keluarannya akan menadi *chipertext* yang tidak bisa dimengerti.

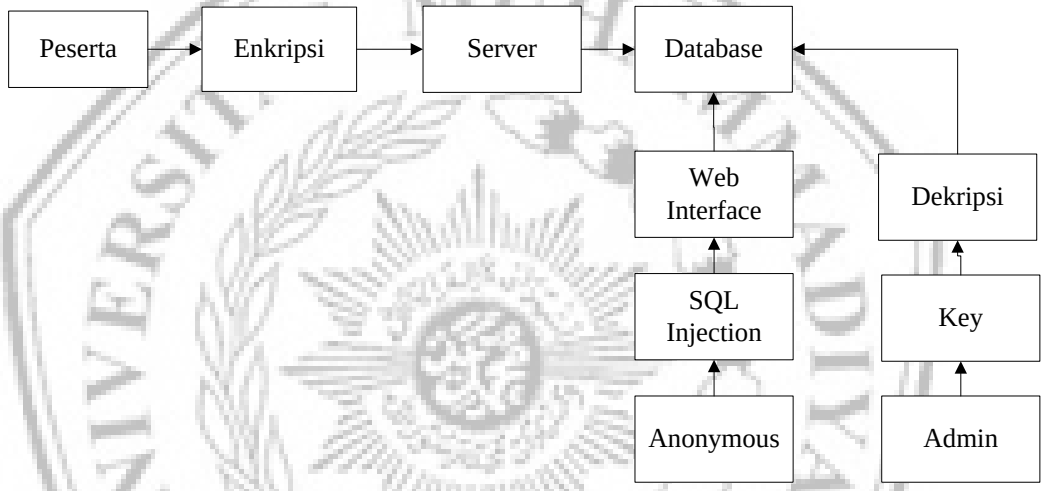
3.5.2 Proses Dekripsi

Berikut adalah diagram blok proses enkripsi nilai ujian:

Gambar 3.5 Diagram Blok Proses Dekripsi Nilai Ujian *Online*

Pada gambar 3.5 dijelaskan bahwa untuk proses dekripsi masukkan berupa *chipertext*. Kemudian akan dilakukan dekripsi dengan algoritma blowfish. Kunci yang digunakan adalah kunci yang sama saat melakukan enkripsi karena algoritma blowfish menggunakan kunci simetris yang mana kunci saat enkripsi dan dekripsi sama. Selanjutnya setelah proses dekripsi berhasil maka keluarannya akan kembali menjadi *plaintext* atau nilai peserta ujian.

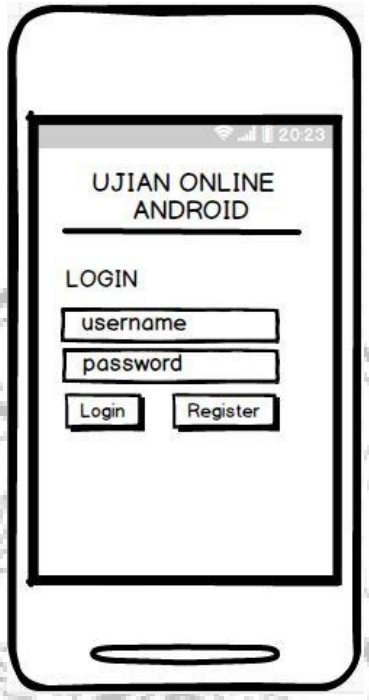
3.6 Perancangan Skenario Penyerangan SQL Injection



Gambar 3.6 Skenario Penyerangan SQL *Injection*

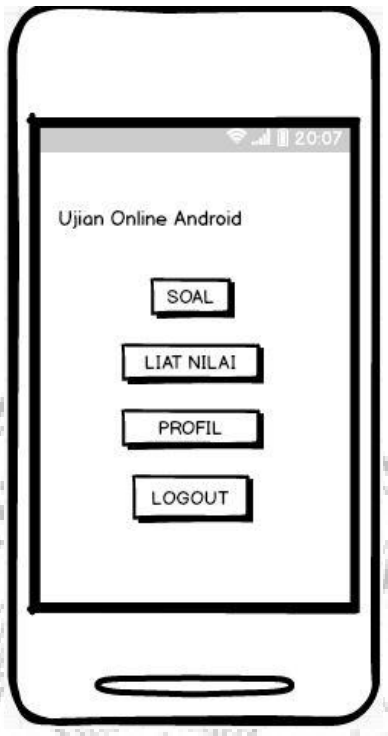
Pada gambar 3.6 Setelah peserta mengerjakan soal, kemudian nilai akan dikirimkan ke server yang telah dienkripsi menggunakan algoritma enkripsi blowfish dan tersimpan dalam database. Dengan menggunakan SQL *Injection* seseorang dapat *login* (masuk) kedalam sebuah *database* tanpa harus memiliki *account*. Disini anonymous akan menyisipkan kode SQL tambahan di form login admin untuk melihat isi database dari form login. Setelah masuk ke dalam database anonymous akan mencoba mengubah nilai peserta yang sudah dilindungi oleh enkripsi Blowfish.

3.7 Desain *Interface*



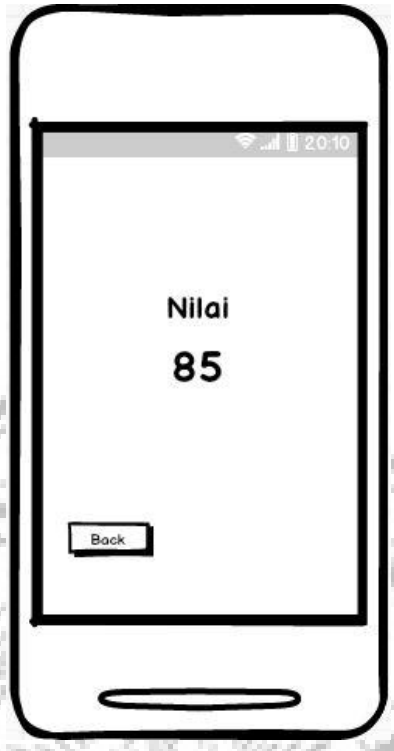
Gambar 3.7 Desain *Interface Form Login*

Gambar 3.8 Desain *Interface Form Register*

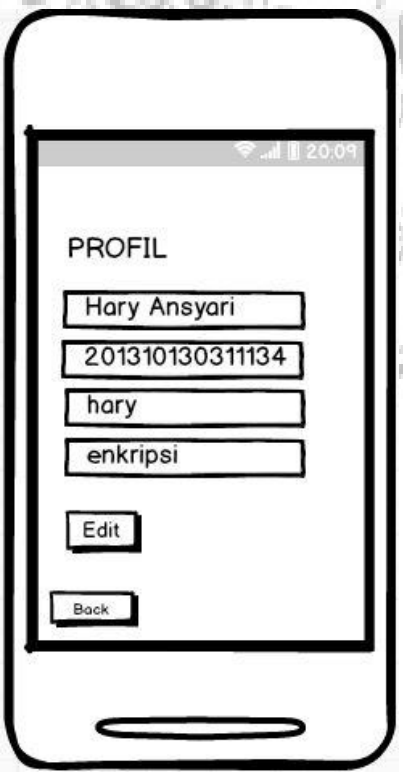


Gambar 3.9 Desain *Interface Menu*

Gambar 3.10 Desain *Interface* Soal Ujian *Online*



Gambar 3.11 Desain *Interface* Nilai Ujian *Online*



Gambar 3.12 Desain *Interface* Profil Peserta Ujian *Online*